

ZFW
AF #

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

GERALD R. MALAN, ET AL.

Serial No.: 09/855,818

Filed: May 15, 2001

Group Art Unit: 2137

Examiner: Shewaye Gelagay

For: METHOD AND SYSTEM FOR PROTECTING PUBLICLY ACCESSIBLE
NETWORK COMPUTER SERVICES FROM UNDESIRABLE NETWORK
TRAFFIC IN REAL-TIME

Attorney Docket No.: UOM 0206 PUSP

APPEAL BRIEF UNDER 37 C.F.R. § 41.37

Mail Stop Appeal Brief - Patents
Commissioner for Patents
U.S. Patent & Trademark Office
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This is an Appeal Brief from the final rejection of claims 1-4, 7-12, and 15-16
of the Office Action mailed on September 7, 2005 for the above-identified patent application.

02/07/2006 MAHME1 00000045 09855818

01 FC:1402

500.00 0P

I. REAL PARTY IN INTEREST

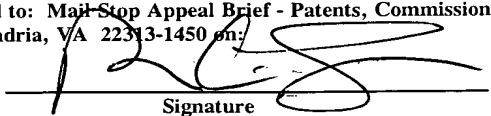
The real party in interest is The Regents of the University of Michigan
("Assignee"), a non-profit corporation organized and existing under the laws of the state of
Michigan, and having a place of business at 3003 S. State Street, Ann Arbor, Michigan 48109,

CERTIFICATE OF MAILING UNDER 37 C.F.R. § 1.8 (FIRST CLASS MAIL)

I hereby certify that this paper, including all enclosures referred to herein, is being deposited with the United States Postal Service as first-class mail, postage pre-paid, in an envelope addressed to: Mail Stop Appeal Brief - Patents, Commissioner for Patents, U.S. Patent & Trademark Office, P.O. Box 1450, Alexandria, VA 22313-1450 on:

February 2, 2006
Date of Deposit

Benjamin C. Stasa
Name of Person Signing


Signature

as set forth in the assignment recorded in the U.S. Patent and Trademark Office on May 15, 2001 at Reel 011816/Frame 0912.

II. RELATED APPEALS AND INTERFERENCES

There are no appeals or interferences known to the Appellant, the Appellant's legal representative, or the Assignee which will directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III. STATUS OF CLAIMS

Claims 1-4, 7-12, and 15-16 are pending in this application. Claims 1-4, 7-12, and 15-16 have been rejected and are the subject of this appeal.

IV. STATUS OF AMENDMENTS

An amendment after final rejection was filed on November 4, 2005, and has been accepted.

V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claim 1 provides a method for protecting publicly accessible network computer services from undesirable network traffic in real-time. (p. 4, ll. 3-6). The method includes receiving network traffic including a stream of service requests destined for the publicly accessible network computer services, (p. 4, ll. 9-10), and generating request statistics including connection statistics and service request distributions based on the stream of service requests. (p. 16, ll. 4-6). The method further includes analyzing the request statistics to identify an undesirable user of the services, and limiting or removing access of the identified undesirable user to the services to protect the services. (p. 4, ll. 10-12).

Independent claim 9 provides a system for protecting publicly accessible network computer services from undesirable network traffic in real-time. (p. 9, ll. 1-4). The

system includes an interface, *e.g.*, DoS Scrubber of Figure 1, for receiving network traffic including a stream of service requests destined for the publicly accessible network computer services. (p. 9, ll. 11-18).

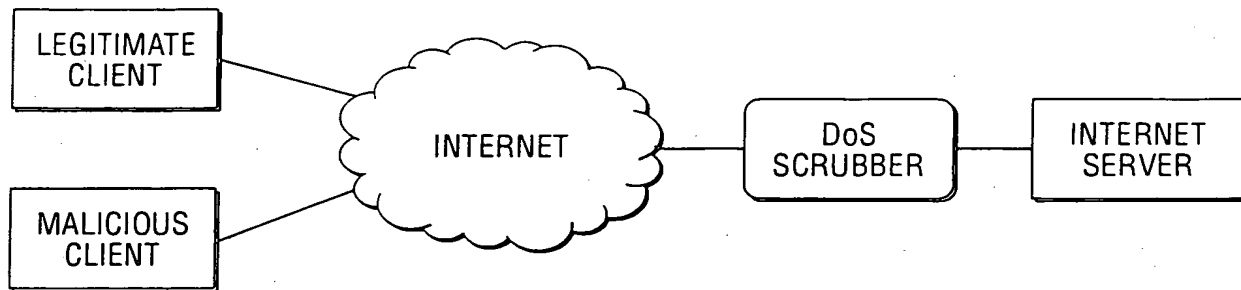


Fig. 1

The system further includes a forwarding engine for generating request statistics including connection statistics and service request distributions based on the stream of service requests, and an analysis engine in communication with the forwarding engine for analyzing the request statistics to identify an undesirable user of the services. (p. 10, ll. 3-8; Figure 2).

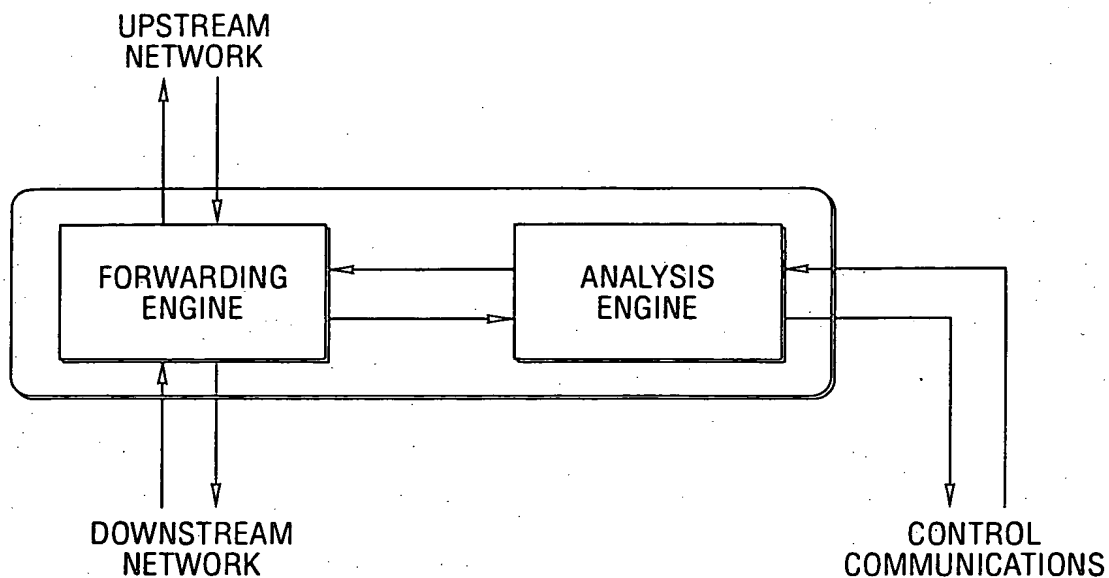


Fig. 2

The forwarding engine limits or removes the access of the identified undesirable user to the services to protect the services. (p. 10, ll. 8-10).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1-4 and 9-12 stand rejected under 35 U.S.C. 103(a) as being unpatentable over U.S. Pat. No. 6,738,814 (Cox) in view of U.S. Pat. No. 4,817,080 (Soha).

Claims 7-8 and 15-16 stand rejected under 35 U.S.C. 103(a) as being unpatentable over Cox in view of Soha and further in view of Smith, R. N., et al. (Smith), "Operating Firewalls Outside the LAN Perimeter".

VII. ARGUMENT

A. Claims 1-4 and 9-12 are not unpatentable under 35 U.S.C. 103(a) over Cox in view of Soha.

Soha discloses a monitoring system for a local-area network. (Abstract). The distributed monitors of Soha examine the packets exchanged between stations connected to a local-area network. (Col. 3, l. 28 - Col. 4, l. 31). With regard to independent claims 1 and 9, Soha does not disclose, teach, or suggest generating request statistics based on a stream of service requests destined for publicly accessible network computer services.

With regard to independent claims 1 and 9, Cox fails to disclose receiving network traffic including a stream of service requests destined for publicly accessible network computer services. Cox instead discloses a routing device receiving packets bound for a private network. (Col. 3, ll. 31-33).

Examiner fails to establish a *prima facie* case of obviousness. For at least the reasons stated above, the references fail to "expressly or impliedly suggest the claimed invention," MPEP § 706.02(j), and Examiner presents no "convincing line of reasoning as

to why the artisan would have found the claimed invention to have been obvious in light of the teachings of the references,” *id.*

Examiner asserts that “one [of] ordinary skill in the art would have been motivated to combine the teachings of Cox with Soha because one would have been motivated as suggested by Cox (Abstract) in order to provide a system to block a network attack based on analyzing network traffic.” (Examiner’s Answer). Cox is directed to a method for blocking denial of service and address spoofing attacks on a private network. In contrast, the invention is directed to a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time. Examiner also asserts that modifying Cox in light of Soha “would have been obvious because a person having ordinary skill in the art would have been motivated as suggested by Soha, (Col. 2, lines 54-57) in order to allow enough statistics of interest to be collected even for the shortest packet independent of the specific information that the user request [sic].” (Office Action Dated 9/7/2005, pp. 5-6). Soha’s statistics of interest are collected from packets exchanged between stations on a local-area network. (Col. 2, ll. 18-20; Col. 3, l. 28 - Col. 4, l. 31). Soha does not teach or suggest that these packets include a stream of service requests destined for publicly accessible network computer services.

Cox discloses a routing device that provides a connection between a private network and an “Internet cloud.” (Col. 2, ll. 48-52). The routing device analyzes packets bound for the private network against known patterns. (Col. 2, l. 67 - Col. 3, l. 35). The distributed monitors connected to the local-area network (LAN) of Soha do not act as routing devices. Soha’s monitors count packets exchanged between the stations of the local-area network. (Col. 4, ll. 26-28). The monitors then send resultant statistics to a monitor manager, which performs higher level processing to generate information placed on a display for users. (Col. 4, ll. 28-31). For at least these reasons, Cox and Soha fail to provide a motivation to combine the references. Moreover, a routing device that analyzes packets bound for a private

network against known patterns (as disclosed by Cox) and LAN- connected monitors that count packets exchanged between the stations of the local-area network (as disclosed by Soha) do not yield a method and system for protecting publicly accessible network computer services from undesirable network traffic in real-time as claimed in claims 1 and 9.

Claims 2-4 and 10-12 depend from claims 1 and 9 respectively. For at least the reasons claims 1 and 9 are not unpatentable over Cox in view of Soha, claims 2-4 and 10-12 are not unpatentable over Cox in view of Soha. Claims 2-4 and 10-12 recite further limitations beyond claims 1 and 9 respectively providing additional reasons why claims 2-4 and 10-12 are not unpatentable over Cox in view of Soha.


B. Claims 7-8 and 15-16 are not unpatentable under 35 U.S.C. 103(a) over Cox in view of Soha and further in view of Smith.

Claims 7-8 and 15-16 depend from claims 1 and 9 respectively. For at least the reasons claims 1 and 9 are not unpatentable over Cox in view of Soha, claims 7-8 and 15-16 are not unpatentable over Cox in view of Soha and further in view of Smith. Claims 7-8 and 15-16 recite further limitations beyond claims 1 and 9 respectively providing additional reasons why claims 7-8 and 15-16 are not unpatentable over Cox in view of Soha and further in view of Smith.

The fee of \$500 as applicable under the provisions of 37 C.F.R. § 41.20(b)(2) is enclosed. Please charge any additional fee or credit any overpayment in connection with this filing to our Deposit Account No. 02-3978.

Respectfully submitted,

GERALD R. MALAN, ET AL.

By: 
Benjamin C. Stasa
Registration No. 55,644
Attorney for Applicants

Date: February 2, 2006

BROOKS KUSHMAN P.C.
1000 Town Center, 22nd Floor
Southfield, MI 48075-1238
Phone: 248-358-4400
Fax: 248-358-3351

Enclosure - Appendices

VIII. CLAIMS APPENDIX

1. A method for protecting publicly accessible network computer services from undesirable network traffic in real-time, the method comprising:

receiving network traffic including a stream of service requests destined for the publicly accessible network computer services;

generating request statistics including connection statistics and service request distributions based on the stream of service requests;

analyzing the request statistics to identify an undesirable user of the services; and

limiting or removing access of the identified undesirable user to the services to protect the services.

2. The method as claimed in claim 1 wherein the undesirable network traffic includes denial of service attacks.

3. The method as claimed in claim 1 wherein the network is the Internet.

4. The method as claimed in claim 1 further comprising generating one or more user profiles from the request statistics wherein the step of analyzing includes the step of comparing the one or more user profiles with a predetermined profile to determine the undesirable user.

7. The method as claimed in claim 1 wherein the network is the Internet and wherein the step of generating request statistics includes the steps of collecting and correlating Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

8. The method as claimed in claim 7 wherein the step of correlating includes the step of identifying a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.

9. A system for protecting publicly accessible network computer services from undesirable network traffic in real-time, the system comprising:

an interface for receiving network traffic including a stream of service requests destined for the publicly accessible network computer services;

a forwarding engine for generating request statistics including connection statistics and service request distributions based on the stream of service requests; and

a analysis engine in communication with the forwarding engine for analyzing the request statistics to identify an undesirable user of the services, the forwarding engine limiting or removing access of the identified undesirable user to the services to protect the services.

10. The system as claimed in claim 9 wherein the undesirable network traffic includes denial of service attacks.

11. The system as claimed in claim 9 wherein the network is the Internet.

12. The system as claimed in claim 9 wherein the forwarding engine generates one or more user profiles from the request statistics and wherein the analysis engine compares the one or more user profiles with a predetermined profile to determine the undesirable user.

15. The system as claimed in claim 9 wherein the network is the Internet and wherein the forwarding engine collects and correlates Border Gateway Protocol (BGP) data from the Internet to obtain the service request distributions.

16. The system as claimed in claim 15 wherein the forwarding engine identifies a topologically clustered set of machines in the Internet based on the data and wherein the service request distributions are generated from the set of machines.

IX. EVIDENCE APPENDIX

None.

X. RELATED PROCEEDINGS APPENDIX

None.